ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 45, Number 4, 2015

ALL FINITE AUTOMORPHIC LOOPS HAVE THE ELEMENTWISE LAGRANGE PROPERTY

PIROSKA CSÖRGŐ

ABSTRACT. An automorphic loop (or A-loop) is a loop whose inner mappings are automorphisms. An open problem was: Does every finite automorphic loop have the elementwise Lagrange property? We give a positive answer to this problem.

1. Introduction. A quasigroup Q that possesses an element 1 satisfying $1x = x1 = x$ for every $x \in Q$ is called a *loop* with neutral element 1. The mappings $L_a(x) = ax$ (*left translation*) and $R_a(x) = xa$ (*right translation*) are permutations of Q for every $a \in Q$. The permutation group generated by left and right translations $\mathrm{Mlt}\,(Q) = \langle L_a, R_a \mid a \in Q\rangle$ is called the *multiplication group* of Q. The *inner mapping group*, $\mathrm{Inn}\,(Q)$ is defined as the stabilizer of 1 in $\mathrm{Mlt}\,(Q)$. A loop Q is commutative if $L_x = R_x$ for every $x \in Q$.

A loop Q is an automorphic loop (or A-loop) if every inner mapping of Q is an automorphism of Q, that is, $\mathrm{Inn}\,(Q) \leq \mathrm{Aut}\,(Q)$. Thus, the class of A-loops, which is certainly not the class of all loops, includes for example groups, commutative Moufang loops [**2**].

The study of A-loops was initiated by Bruck and Paige [**3**]. Further remarkable results concerning A-loops can be found in [**7, 9**]. In [**6**], Jedlička, Kinyon and Vojtěchovský studied the structural properties of commutative A-loops. Among other results, they examined the commutative A-loops of odd order. One of their main results is the odd order theorem: every commutative A-loop of odd order is solvable

2010 AMS *Mathematics subject classification.* Primary 08A05, 20N05.

Keywords and phrases. A-loop, elementwise Lagrange property, multiplication group, inner mapping group, connected transversals.

This paper was partially supported by Hungarian National Foundation for Scientific Research grant No. K84233.

Received by the editors on January 22, 2012, and in revised form on March 25, 2013.

DOI:10.1216/RMJ-2015-45-4-1101

([**6,** Theorem 3.12]). They showed the Lagrange and Cauchy theorems for commutative A-loops of odd order ([**6,** Propositions 3.6 and 3.7]).

In [**4, 8**], the authors showed the nilpotency of commutative automorphic p-loops of odd order and that their multiplication groups are p-groups. A new result is the solvability of all automorphic loops of odd order (see [**10**]).

Bruck and Paige [**3**] established the power associativity of A-loops, that is, each 1-generated subloop $\langle a\rangle$ is, in fact, a cyclic group. This makes sense to study the following open problem: Does every finite automorphic loop have the elementwise Lagrange property?

We give a positive answer to this problem. We are working in the multiplication group of the automorphic loop. Our proof is completely group theoretical. We prove our result by applying the theory of connected transversals. This concept was introduced by Niemenmaa and Kepka [**11**]. Using their characterization theorem, we can transform loop theoretical problems into group theoretical problems.

2. Basic definitions and results. For the basic concepts of loop theory we refer to Bruck [**1**]. Here we review some definitions, notations and results.

Let Q be a loop. Set $A = \{L_c \mid c \in Q\}$ and $B = \{R_d \mid d \in Q\}$. Then A and B are left transversals to $\mathrm{Inn}\,(Q)$ in $\mathrm{Mlt}\,(Q)$, $\langle A, B\rangle = \mathrm{Mlt}\,(Q)$, $[A, B] \le \mathrm{Inn}\,(Q)$ and $\mathrm{core}_{\mathrm{Mlt}\,(Q)}\mathrm{Inn}\,(Q) = 1$ (i.e., the largest normal subgroup of $\mathrm{Mlt}\,(Q)$ in $\mathrm{Inn}\,(Q)$ is trivial). As a consequence, $A \cap \mathrm{Inn}\,(Q) = B \cap \mathrm{Inn}\,(Q) = 1$ holds.

Conversely, consider a group G with the following properties: H is a subgroup of G, A and B are left transversals to H in G. A and B are *H-connected transversals* by definition, if $[A, B] \le H$.

By a result of Kepka and Niemenmaa [**11**], the above two situations are equivalent:

Theorem 2.1. *A group G is isomorphic to the multiplication group of a loop if and only if there is a subgroup H, for which there exist H-connected transversals A and B such that $\langle A, B\rangle = G$ and* $\mathrm{core}_G H = 1$.

Let Q be a loop and S a normal subloop of Q. By [**5,** Proposition

1.2] we have $\mathrm{Inn}\,(Q)$ acts on S. Using $\mathrm{Mlt}\,(Q) = A \cdot \mathrm{Inn}\,(Q)$, it follows that S is a block of $\mathrm{Mlt}\,(Q)$ which contains the neutral element. Hence, S corresponds to the subgroup $\mathcal{M}(S)\mathrm{Inn}\,(Q)$ where $\mathcal{M}(S) = \langle L_s, R_s \mid s \in S\rangle$. Put $K(S) = \mathrm{core}_{\mathrm{Mlt}\,(Q)}\,(\mathcal{M}(S)\mathrm{Inn}\,(Q))$. Denote by f the natural homomorphism of $\mathrm{Mlt}\,(Q)$ onto $\mathrm{Mlt}\,(Q)/K(S)$. Then $f(A)$ and $f(B)$ are $f(\mathrm{Inn}\,(Q))$-connected transversals in $\mathrm{Mlt}\,(Q)/K(S)$ (see [**11,** Lemma 2.5 and Lemma 2.8]) and for the multiplication group of the factorloop Q/S the following is true: $\mathrm{Mlt}\,(Q/S) \cong \mathrm{Mlt}\,(Q)/K(S)$.

The permutation group generated by all left translations is called the left multiplication group, and we shall denote it by $\mathcal{L} = \mathcal{L}(Q) = \langle A\rangle$. In a similar way, the right multiplication group $\mathcal{R} = \mathcal{R}(Q) = \langle B\rangle$ is generated by all right translations. Let $\mathcal{L}_1 = \mathcal{L} \cap \mathrm{Inn}\,(Q)$, and $\mathcal{R}_1 = \mathcal{R} \cap \mathrm{Inn}\,(Q)$.

Lemma 2.2. $\mathrm{Aut}\,(Q) \cap \mathrm{Inn}\,(Q) = \mathrm{Inn}\,(Q) \cap N_{\mathrm{Mlt}\,(Q)}(A) = \mathrm{Inn}\,(Q) \cap N_{\mathrm{Mlt}\,(Q)}(B)$, *i.e.,*

$$\mathrm{Inn}\,(Q) \le \mathrm{Aut}\,(Q) \textit{ if and only if}$$
$$\mathrm{Inn}\,(Q) \le N_{\mathrm{Mlt}\,(Q)}(A) \cap N_{\mathrm{Mlt}\,(Q)}(B).$$

Proof. See [**4,** Lemma 2.3]. □

3. A-loops. Let Q be an A-loop. $A = \{L_x \mid x \in Q\}$, $B = \{R_x \mid x \in Q\}$. Denote $G = \mathrm{Mlt}\,(Q)$, $H = \mathrm{Inn}\,(Q)$. We have $G = \langle A, B\rangle$, $[A, B] \le H$, $\mathrm{core}_G H = 1$ (see Theorem 2.1). As $H \le \mathrm{Aut}\,(Q)$,$H \le N_G(A) \cap N_G(B)$ by Lemma 2.2.

Lemma 3.1. *Let $h \in H$, $\alpha \in A$ be such that $h^\alpha \in H$. Then $\alpha \in C_G(h)$. (Similarly, if $h \in H$, $\beta \in B$ such that $h^\beta \in H$. Then $\beta \in C_G(h)$.)*

Proof. $h \in N_G(A)$ implies $\alpha^h = \alpha_1$ with $\alpha_1 \in A$. Hence, $h^\alpha = h\alpha_1^{-1}\alpha \in H$. As A is a left transversal to H, $\alpha = \alpha_1$ follows, i.e., $\alpha \in C_G(h)$.

(In a similar way $\beta \in C_G(h)$.) □

Lemma 3.2. *$H \cap C_G(A) = H \cap C_G(B)$.*

Proof. From Lemma 3.1, it is obvious. □

Proof. Denote $a = L_x$ and $b = R_x$. We have $b = ah$ with $h \in H$. As $[a, b] \in H$, $a^h \in aH$ holds, whence $h^a \in H$. By using Lemma 3.1, it follows that $a \in C_G(h)$; consequently, $a \in C_G(b)$ is true. □

Theorem 3.3. *Let Q be a finite automorphic loop. Then Q has the elementwise Lagrange property, i.e., the order of any element of Q is the divisor of the order of Q.*

Proof. Assume there is an element x of $Q \setminus \{1\}$ such that $o(x) = t$ and t is not the divisor of $|Q|$.

Let $G = \operatorname{Mlt} Q$, $H = \operatorname{Inn} Q$. We have $|Q| = |G : H|$.

Let $a = L_x$, $b = R_x$. As $o(x) = t$, t is the minimal natural number that $a^t \in H$ and $b^t \in H$. We have that t is not the divisor of $|Q|$, whence it follows that there exists a prime divisor p of t such that $t = rp^l$ with $(r, p) = 1$, and p^l is not the divisor of $|Q|$.

Let $P_0 \in \operatorname{Syl}_p(H)$ and $P \in \operatorname{Syl}_p(G)$ such that $P \geq P_0$. We have $|P : P_0| = p^k$ with $k \geq 0$; hence, p^k is the divisor of $|G : H|$. Consequently, $k < l$.

Clearly, there exists a natural number j such that $a^j \in G \setminus H$, a^j is a p-element and p^l is the minimal power of p with $a^{jp^l} \in H$. By using Sylow's theorems, we get that there exists $g_0 \in G$ such that $(a^j)^{g_0} \in P$. As $|P : P \cap H| = |P : P_0| = p^k$, we have $(a^{jp^m})^{g_0} \in P \cap H$ for some $0 \leq m \leq k$. Since $G = BH$, then $g_0 = b_0 h_0$ with $b_0 \in B$, $h_0 \in H$. Hence, $(a^{jp^m})^{b_0} \in H$.

Obviously $a^{b_0} \in C_G(a^{jp^m})^{b_0}$. $[A, B] \leq H$ implies $a^{b_0} = ah$ with $h \in H$, and $(a^{jp^m})^{b_0 a} = (a^{jp^m})^{b_0 h^{-1}} \in H$ follows. Applying Lemma 3.1, we get $a \in C_G(a^{jp^m})^{b_0}$.

As $0 \leq m \leq k < l$ and p^l is the minimal power of p such that $a^{jp^l} \in H$, we get $(a^{jp^m})^{b_0} \neq e$; consequently, $C_G(a) \cap H$ has a p-element.

Let P^* be an abelian p-subgroup of maximal order in H such that $a \in C_G(P^*)$. Since $a^j \in C_G(P^*)$ and a^j is a p-element it follows that $T = \langle P^*, a^j \rangle$ is an abelian p-subgroup. By using the properties of a^j we can conclude $|T : T \cap H| = p^l$. Sylow's theorem implies that there exists $g_1 \in G$ such that $T^{g_1} \leq P$.

Clearly, $a^{g_1} \in C_G(T^{g_1})$. Since $|P : P \cap H| = p^k$ and $P \cap H = P_0 \in \mathrm{Syl}_p(H)$ it follows that $|T^{g_1} : T^{g_1} \cap H|$ is a divisor of p^k. $G = BH$ implies $g_1 = b_1 h_1$ with $b_1 \in B$, $h_1 \in H$. We have $a^{g_1} \in C_G(T^{g_1} \cap H)$, whence $a^{b_1} \in C_G(T^{g_1} \cap H)^{h_1^{-1}}$. Using $a^{b_1} = ah^*$ and $h^* \in H$, we get $(T^{g_1} \cap H)^{h_1^{-1}a} = (T^{g_1} \cap H)^{h_1^{-1}(h^*)^{-1}} \leq H$. Again applying Lemma 3.1, it follows that $a \in C_G(T^{g_1} \cap H)^{h_1^{-1}}$.

As $|T : T \cap H| = p^l$ and $|T^{g_1} : T^{g_1} \cap H|$ is a divisor of p^k, $k < l$ implies $|T^{g_1} \cap H| \gneqq |T \cap H|$. Hence, $|(T^{g_1} \cap H)^{h_1^{-1}}| \gneqq |T \cap H| \geq |P^*|$. We have $a \in C_G(T^{g_1} \cap H)^{h_1^{-1}}$, which contradicts the maximality of $|P^*|$. □

REFERENCES

1. R.H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

2. ———, *A survey of binary systems*, Springer-Verlag, New York, 1971.

3. R.H. Bruck and L.J. Paige, *Loops whose inner mappings are automorphisms*, Ann. Math. **63** (1956), 308–323.

4. P. Csörgő, *Multiplication groups of commutative automorphic p-loops of odd order are p-groups*, J. Alg. **350** (2012), 77–83.

5. A. Drápal, *Conjugacy closed loops and their multiplication groups*, J. Alg. **272** (2004), 838–850.

6. P. Jedlička, M.K. Kinyon and P. Vojtěchovský, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), 365–384.

7. ———, *Constructions of commutative automorphic loops*, Comm. Alg. **38** (2010), 3243–3267.

8. ———, *Nilpotency in automorphic loops of prime power order*, J. Alg. **350** (2012), 64–76.

9. M.K. Kinyon, K. Kunen, J.D. Phillips and P. Vojtěchovský, *Every diassociative* A*-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), 619–624.

10. ———, *The structure of automorphic loops*, in preparation.

11. M. Niemenmaa and T. Kepka, *On multiplication groups of loops*, J. Algebra **135** (1990), 112–122.

Eötvös University, Department of Algebra and Number Theory, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary
Email address: ska@cs.elte.hu